PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-060947
(43)Date of publication of application : 06.03.2001

(51)Int.Cl. H04L 9/32
G06F 15/00
H04L 9/08

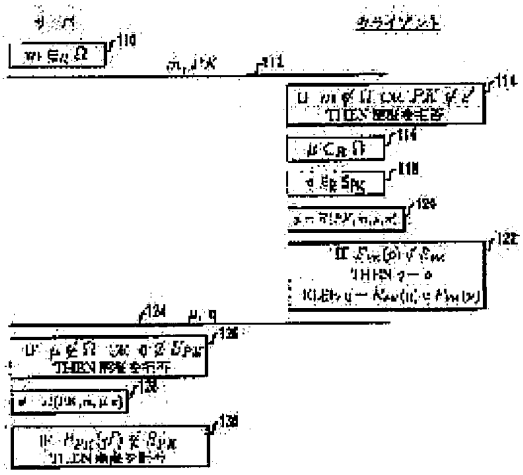
(21)Application number : 2000-210117
(22)Date of filing : 11.07.2000

(71)Applicant : LUCENT TECHNOL INC
(72)Inventor : MACKENZIE PHILIP DOUGLAS
SWAMINATHAN RAM

(30)Priority
Priority number : 99 353468 Priority date : 13.07.1999 Priority country : US

(54) MUTUAL NETWORK AUTHENTICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a password single mutual authentication protocol which can prove safety.
SOLUTION: A client decides whether a public key received from a server is the element of the test possible super set of the set of all public keys in a public key cipher system. When it is not such element, authentication is refused by the client. If not, a protocol is continued. In one embodiment, the client and the server shares one password used for authentication. The client generates a parameter (p) as the function of at least the public key and the password. When, as a result of operating a public key space mapping function FPK to (p), the FPK is the element of the message space of the public key, the client uses the open key to cipher the substantially random element in the message space of the public key and executes the group operation of the public key message space between the ciphered result and the FPK (p).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－60947
（P2001－60947A）
(43)公開日　平成13年３月６日(2001.3.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ	9/00	６７３Ａ
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｅ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ	9/00	６０１Ｃ
				６７５Ｂ

審査請求　未請求　請求項の数66　ＯＬ　（全 16 頁）

(21)出願番号　特願2000－210117(P2000－210117)

(22)出願日　平成12年７月11日(2000.7.11)

(31)優先権主張番号　０９／３５３４６８

(32)優先日　平成11年７月13日(1999.7.13)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　596077259
ルーセント　テクノロジーズ　インコーポレイテッド
Ｌｕｃｅｎｔ　Ｔｅｃｈｎｏｌｏｇｉｅｓ　Ｉｎｃ．
アメリカ合衆国　07974　ニュージャージー、マレーヒル、マウンテン　アベニュー　600－700

(74)代理人　100081053
弁理士　三俣　弘文

最終頁に続く

(54)【発明の名称】　相互ネットワーク認証方法